BY ORDER OF THE COMMANDER
AIR FORCE SPECIAL OPERATIONS
COMMAND

AIR FORCE SPECIAL OPERATIONS
COMMAND INSTRUCTION 33-202

11 AUGUST 2011

Communications and Information

PORTABLE ELECTRONIC DEVICE (PED) SECURITY

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available for downloading or ordering on the e-Publishing website at **www.e-Publishing.af.mil.**

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: HQ AFSOC/A6OI

Certified by: HQ AFSOC/A6O
(Lt Col Charmaine Martin)

Supersedes: AFSOCI 33-202,
31 March 2004

Pages: 17

This instruction implements DODI 5200.1-R, *DoD Information Security Program and Protection of Sensitive Compartmented Information*, 9 Oct 2008; AFI 33-112, *Information Technology Hardware Asset Management*, 7 Apr 2006; AFI 33-219, *Telecommunications Monitoring and Assessment Program*, 1 May 2006; AFI 33-322, *Records Management Program,* 7 Oct 2003; AFMAN 33-223, *Identification and Authentication,* 6 Jul 2006; and AFMAN 33-363, *Management of Records,* 8 Mar 2008. This instruction applies to active duty AFSOC units and all individuals working on an AFSOC installation. It does not apply to the Air Force Reserve Command (AFRC) or the Air National Guard (ANG). Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of in accordance with Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS) located at **https://www.my.af.mil/afrims/afrims/afrims/rims.cfm**. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the Air Force (AF) Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the appropriate functional's chain of command.

SUMMARY OF CHANGES

This revision updates the AFSOC policy and guidance concerning portable electronic device security.

1. Purpose. This instruction provides AFSOC personnel guidance on the proper use of PEDs. The guidance includes security measures to ensure the integrity and security of AFSOC information and systems. The policy incorporates directives from DOD, USSOCOM, and AF into a single directive to reduce the number of policies users must access to locate applicable guidance.

1.1. **PEDs include:**

1.1.1. Personal Digital Assistants (PDA).

1.1.2. Tablet Personal Computers (PCs).

1.1.3. Laptop/netbook computers.

1.1.4. Cellular telephones (CT).

1.1.5. Two-way pagers.

1.1.6. Digital imagery/recording cameras devices (still and/or video).

1.1.7. Wireless PDA/email devices (e.g., Research in Motion's Blackberry devices/Smartphones).

1.1.8. Secure Mobile Environment Portable Electronic Devices (SME PEDs)

1.1.9. Any other devices of similar capability or design.

1.2. **PEDs exclude:**

1.2.1. Land mobile radios (LMRs).

1.2.2. Emergency radios.

1.2.3. Tactical radios.

1.2.4. One-way, receive-only devices (such as receive-only pagers).

1.2.5. Devices that only play prerecorded media.

1.3. This policy will be reviewed and updated, as required, to address technology changes that may provide practical application for the command without introducing unacceptable security risks and vulnerabilities.

2. Scope. This policy is applicable to all PEDs used within AFSOC facilities/organizations regardless of the type, classification, or functionality. References to PEDs are government procured/owned, unless otherwise specified.

3. Applicability. This instruction applies to active duty AFSOC units and all individuals working on an AFSOC installation. It does not apply to the Air Force Reserve Command (AFRC) or the Air National Guard (ANG). AFSOC units/geographically separated units (GSUs)/bases will augment this policy with local policy. Organizations may make their policy more restrictive, but in no case less restrictive. When AFSOC policy is in conflict with AFIs or USSOCOM/local policy, the more restrictive policy will be followed. Failure to adhere to the provisions of this instruction may result in termination of network access to all AFSOC and/or DOD supported networks and in other disciplinary and legal penalties, as appropriate.

4. Background. The proliferation of PEDs within the AFSOC Enterprise is expanding rapidly. While providing productivity benefits, the ability of these devices to store and transmit classified information through both wired and wireless networks poses potential risks to an organization's security. Particularly, their potential use in and around areas where classified information may be discussed or processed creates new risks of which commanders and users must be made aware. PEDs providing wireless capabilities pose even greater challenges by increasing the risk of compromising emanations. A balance between security and functionality is required to maximize the benefits derived from PEDs while preserving the ability to conduct secure discussions, meetings, and communications. This instruction establishes a minimum standard security posture for PEDs and provides AFSOC Designated Approving Authorities (DAA), Unit Commanders, and Information System Security Officers (ISSOs), a framework from which local PED policy and directives can be derived.

5. Responsibilities.

5.1. HQ AFSOC/A6O. Serves as the OPR for this instruction and updates it when required.

5.2. Building Facility Managers. Posts signs at strategic entry/exit locations where PED use is not authorized. See Attachment 2 for an example sign.

5.3. Unit Commanders.

5.3.1. Designate facilities or rooms where PED use is unauthorized.

5.3.2. Except for cellular telephones with no PDA capability, purchase only PEDs that have received an AFSOC CTO.

5.3.3. Ensure an ISSO is appointed to facilitate processing/handling PED security requirements.

5.4. Unit ISSOs.

5.4.1. Provide PED users security training utilizing Attachment 3 as a guide. Units may develop local training material, but must include the topics in Attachment 3 as a minimum.

5.4.2. Provide PED users periodic updates on security issues.

5.4.3. Act as the unit's single focal point for handling/resolving PED security issues.

5.5. Client Systems Technician (CST). The following statements apply only to government owned PEDs that process or store data (e.g., PDAs or cellular phones with PDA capabilities) or connect to the base network either directly or indirectly through "hot-syncing" with a desktop workstation.

5.5.1. Are the user's focal point for resolving any technical issues/problems.

5.5.2. Configure PED operating systems and applications to ensure compliance with this policy.

5.5.3. Install antivirus software, when applicable, on PEDs and associated workstations.

5.5.4. Notify PED users when a software upgrade or maintenance is required.

5.5.5. Provide antivirus and security software sourcing information and initial technical support for government owned PEDs (e.g., assisting a user accessing e-mail using Outlook Web Access (OWA)).

5.6. Meeting/Conference hosts/OPRs. Responsible for reminding users to appropriately secure PEDs prior to the start of meetings where classified information may be processed, discussed, or viewed.

5.7. Base Equipment Control Officer (BECO)/ Equipment Custodians.

5.7.1. Centrally track and account for PED device ownership in accordance with AFI 33-112, *Information Technology Hardware Asset Management*, and local BECO policies.

6. Facility Policy. Those facilities/rooms commanders have identified as PED restricted must identify which types of PEDs are prohibited and coordinate with Facility Managers to post signs accordingly.

7. PED Policy. Effective immediately, any new PEDs used within AFSOC shall be in accordance with the following policy. **Exception:** Those individuals/units who are already using PEDs shall comply with this policy where technically possible and must develop and execute a conformance plan to ensure 100% compliance within 90 days.

7.1. General. Policy for all classes of PEDs.

7.1.1. PEDs that connect to the base network (via direct or wireless access, through a docking station, or via any other connection means) must use operating systems and applications that have been approved, certified, and accredited by the Chief Information Officer (CIO) and DAA to ensure they meet minimum technical and security requirements for the supported business or mission and are compliant with AFSOC and host base's certification and accreditation rules.

7.1.2. Wireless PEDs will not be used for storing, processing, or transmitting classified information unless specifically authorized by the cognizant authority (*DAA for data devices and unit commander for voice-only devices).* If approved by the DAA, then only assured channels employing National Security Agency (NSA) approved, Type-1 end-to-end encryption will be used to transmit classified information. PEDs (and any connected storage media) shall be safeguarded in accordance with DOD Instruction 5200.1-R, DOD

INFORMATION SECURITY PROGRAM AND PROTECTION OF SENSITIVE COMPARTMENTED INFORMATION

7.1.3. AFSOC personnel:

7.1.3.1. When utilizing PEDs, users shall use good operations security (OPSEC), shall protect classified data from disclosure to unauthorized parties, and shall refrain from any practices that might jeopardize, compromise, or render useless any garrison and/or tactical AFSOC data, system, or network.

7.1.3.2. Are individually responsible and liable for any disclosures of classified information if the member/employee sends such information through a PED.

7.1.3.3. Shall not transmit classified data or information through a PED unless specifically authorized by the cognizant authority. **Note:** All classified data transfers shall be performed only on fully accredited, classified systems.

7.1.3.4. Shall not use the PED to access the Internet or E-mail services that are not provided by the host base when it is connected to an AFSOC workstation (e.g., the PED's wireless capability is still on and providing a back-door network connection to a commercial web site).

7.1.3.5. May not use unofficial E-mail services for official business without the expressed permission of the DAA.

7.1.3.6. Shall notify the Wing Information Assurance Office (WIAO) immediately upon discovery or suspicion of classified compromise on PEDs or operation of PEDs counter to the security provisions of this instruction that could result in compromise of classified information.

7.1.4. PEDs that process and store data are considered Information Systems (IS) and must be configured, managed, and controlled in accordance with local IS procurement, inventory, control, and disposition policy and procedures.

7.1.5. Operation of PEDs with radio frequency **(**RF)/wireless, Infrared (IR), and audio/video record capabilities is not permitted within 5 meters of Continental United States (CONUS) and 10 meters of Outside the Continental United States (OCONUS) (*hereto after referred to as "exclusion zones"*) designated AFSOC organizations/spaces where classified information is processed, discussed, or transmitted unless specifically authorized by the cognizant authority. If approval is granted, the device's RF/wireless, IR, and audio/video record capabilities shall be disabled while inside of these areas.

7.1.6. No PEDs, regardless of government or private ownership, or wireless/non-wireless capability, will be permitted within any AFSOC permanent, temporary, or mobile Sensitive Compartmented Information Facilities (SCIF), Special Access Program (SAP), or Special Access Required (SAR) facilities without prior written approval of the cognizant Senior Intelligence Officer (SIO) or SAP/SAR Security Manager respectively. If approval is granted, RF, IR, and audio/video capabilities must be disabled. All PEDs will be declared to the SSO or SAP Security Manager, respectively, before entry into a SCIF, SAP, or SAR facility.

7.1.7. All PED software (operating system, applications, etc.), must have a valid Certificate to Operate (CTO) and authority to connect (ATO) (DAA approval). This ensures they have been determined to be compliant with applicable National Telecommunications and Information Administration (NTIA) and Federal Communications Commission (FCC) requirements and have the technical ability to comply with this AFSOCI.

7.1.8. Users should not attempt to block sending and receiving features using any method that has not been approved by the DAA.

7.1.9. AFSOC members/employees shall ensure that their use of such devices does not lead to loss or exposure of classified information.

7.1.10. PED users shall exercise positive physical security over their devices to minimize the risk of compromising information resulting from the loss or theft of such devices.

7.1.11. PED users shall report any suspicious activity involving their devices to their respective ISSO.

7.1.12. Information maintained on PEDs (e.g., original copies of E-mail messages, Word documents, Excel spreadsheets, etc), like all electronic documents, may be considered official records and may be subject to the provisions of AFI 33-322, *Records Management Program*. **Note:** The original copy of official records should not be stored on the PEDs.

7.1.13. Only AFSOC procured third party network services subscriptions (e.g., AT&T Wireless data network access via a Global System for Mobile Communications (GSM)/Global Packet Radio Service (GPRS) modem and approved application software) will be permitted on government PEDs.

7.2. PED Use within Exclusion Zones. In addition to paragraph 7.1., the following are the minimum requirements when using PEDs inside exclusion zones or inside of AFSOC organizations/spaces that store, process, or transmit classified information. Disabling techniques are listed from most to least secure.

7.2.1. Disable IR Port. The IR port of all PEDs will be disabled using at least one of the following methods in order of precedence. Perform multiple steps simultaneously where possible.

7.2.1.1. If the PED is equipped with a manual switch, position the switch to the disable or off position.

7.2.1.2. Use the PED software feature to turn off the IR port.

7.2.1.3. Cover the IR port completely with aluminum or copper foil tape.

7.2.1.4. If feasible, have the IR capability physically disabled at the factory by the manufacturer.

7.2.2. Wireless Capability. Disable wireless capabilities within the previously defined exclusion zones. PED’s wireless capabilities must be disabled in one of the following methods in order of precedence. Perform multiple steps simultaneously where possible.

7.2.2.1. Physically remove any devices (e.g., compact flash cards, multimedia cards, expansion sleeves, memory sticks, etc) that provide wireless capabilities.

7.2.2.2. Turn off the wireless capability using a built-in hardware switch.

7.2.2.3. Turn off the wireless capability using a software function controlled with a password.

7.2.3. Record Capability. Most PEDs have audio or video record capabilities either built-in or via the use of optional expansion devices. Use at least one of the following methods in order of precedence to disable the record capability. Perform multiple steps simultaneously where possible.

7.2.3.1. Physically remove any devices (e.g., compact flash cards, multimedia cards, expansion sleeves, memory sticks, etc) that provide audio or video recording (either moving picture or still shot photo) capabilities.

7.2.3.2. If the PED is equipped with a manual switch, position the switch to the off position to disable the microphone/camera.

7.2.3.3. Deprogram PED "hot keys" to avoid accidental audio or video recording.

7.2.3.4. Use the PED software feature to turn off the recording capability.

7.2.3.5. Purchase a PED that does not have a record capability.

7.2.4. Control Procedures. All PEDs that process and store government data (*e.g., PDAs*) will be centrally managed by unit workgroup managers to ensure each device has been loaded with the most current anti-virus and encryption software and is properly configured in accordance with this policy for use in an AFSOC facility. The following procedures must be followed when acquiring new PEDs:

7.2.4.1. Only government procured, certified, and accredited PDA devices may be connected to AFSOC unclassified or classified computers/networks after being reviewed and approved by the cognizant ISSO.

7.2.4.2. Where possible, affix a standard form classification label (SF 706 – SF 710) to government PEDs and any external storage devices (e.g., compact flash cards, multimedia cards, memory sticks, expansion sleeves, etc.) to identify the highest classification level of the data processed/stored on the PED. **Note:** The label should be affixed so as to not draw any unnecessary attention to the device.

7.3. Policy for private/corporate owned PEDs. In addition to requirements outlined in paragraph 7.1., and paragraph 7.2., privately owned PEDs must meet the following requirements:

7.3.1. Users are not authorized to connect a private/corporate PED to any AFSOC network. **Note:** This restriction does not apply to users accessing e-mail via Microsoft's Outlook Web Access (OWA) application.

7.4. Policy for Personal Digital Assistants (PDA). In addition to the requirements outlined in Paragraphs 7.1., 7.2., and 7.3., PDAs must meet the following additional requirements:

7.4.1. The SME PED is the only PDA authorized to be connected to a classified computer/network or process/maintain classified information. Under no circumstances will synchronization software be loaded onto computer systems processing classified information.

7.4.2. PDA devices cannot connect wirelessly while connected to the enterprise network. Users will only connect to commercial internet service provider (ISPs) for the explicit purpose of creating a secure connection to the AFSOC enterprise network (i.e. via a Virtual Private Network (VPN)). Additionally, third-party commercial e-mail accounts such as GMail, Hotmail, etc., are not authorized on government furnished PEDs.

7.4.3. Information can be synchronized between a PDA and government workstation/laptop by using an NSA approved tether. The only authorized connection through a PDA modem is to an official Air Force account protected by an authorized Network Control Center firewall.

7.4.4. The following applies to handling and controlling of PDAs:

7.4.4.1. PDAs must identify and authenticate users in accordance with AFMAN 33-223, *Identification and Authentication*, if technically possible. If the PDA is technically unable to use a password, increase physical access controls to prevent unauthorized access.

7.4.4.2. Turn off PDA when not in use.

7.4.5. All government-owned PDA devices will:

7.4.5.1. Utilize "password-locking" utilities or file system encryption software to protect against the loss of sensitive information in accordance with AFM 33-223.

7.4.5.2. Have DOD-approved anti-virus software installed. To ensure consistent levels of protection against viruses, PDAs will maintain up-to-date signature files used to profile and identify viruses, worms, and malicious code. Anti-virus software and updates are available from the DOD Computer Emergency Response Team (CERT) web site (**http://www.cert.mil**).

7.4.5.3. Identify and authenticate users in accordance with AFM 33-223. Where technically capable, passwords will not include words found in the dictionary and will be at least eight characters including upper and lower case letters, numbers, and special characters. Passwords will be changed at least every 90 days on unclassified devices or every 60 days on classified devices in accordance with AFM 33-223. The password protection feature will not permit its bypass without zeroing all data stored on the device.

7.4.5.4. Not be connected at any time (either wired or wireless) to privately owned computer equipment.

7.4.5.5. Where technically capable have a DOD logon banner in accordance with AFI 33-219.

7.5. Policy for Cellular Telephones (CT) and other radio frequency (RF) emitting PEDs. In addition to the requirements outlined in paragraphs 7.1., 7.2., and 7.3., cellular/mobile telephones and RF transmitting PEDs must meet the following additional requirements:

7.5.1. Nonsecure CTs and other RF emitting PEDs are not authorized within exclusion zones unless specifically authorized by the cognizant authority. If approval is granted, the device's RF/wireless, IR, and audio/video record capabilities shall be disabled while inside of these areas. **Note:** Only NSA-approved Type 1 cellular phones, satellite phones, or SME PEDs will be used for classified data, voice, or wireless telephone or data transmissions. The classification level of information transmitted will not exceed the classification level approved for the device.

7.6. Policy for two-way wireless PDA/e-mail devices (e.g., Research in Motion's (RIM) Blackberry devices/smartphones). In addition to the requirements outlined in paragraphs 7.1., 7.2., 7.3., 7.4., and 7.5., two-way wireless PDA/e-mail devices must meet the following additional requirements.

7.6.1. Devices will not be connected to any AFSOC classified computer/network unless specifically approved by the local DAA to meet a specific mission critical need.

7.7. Policy for Two-way pagers. In addition to the requirements outlined in paragraphs 7.1., 7.2., 7.3., and 7.5., two-way pagers must meet the following additional requirements.

7.7.1. Government procured two-way pagers must operate in a receive-only mode or be turned off while in designated AFSOC organizations/spaces where classified information is discussed or processed unless specifically authorized by the cognizant authority.

7.7.2. Privately owned or corporate two-way pagers, approved for use by the cognizant authority, can only be used in a receive-only mode or turned off when in an AFSOC facility/space where classified is discussed or processed.

7.7.3. Two-way pagers will not be permitted in AFSOC permanent, temporary, or mobile SCIF or SAPF unless specifically authorized by the cognizant SIO or SAP Security Manager respectively.

7.8. Policy for SCIFs. The use of PED's in an SCI environment presents an additional risk for the compromise of classified information. PED's will only be used to fulfill mission requirements. Specific handling procedures contained within *Concept of Operations for HQ AFSOC, Special Security Office, Revision 3*, must be strictly adhered to. The Agency in charge of any given SCIF is the authority for the procedures to move PED's in or out of their facilities. In addition to the requirements set forth in paragraphs 7.1., and 7.2., specific requirements/ procedures that must be satisfied prior to approving the use of portable electronic devices within SCIFs are:

7.8.1. Government owned PED's.

7.8.1.1. Hardware, software, and storage media must be controlled when entering/exiting a SCIF.

7.8.1.2. Are prohibited from operating within a SCIF unless authorized and accredited by the agency granting the SCIF accreditation or delegated authority such as the ISSO. As part of the accreditation requirements, the user of these devices and his/her supervisor must sign a statement acknowledging that they understand and will adhere to the restrictions identified below.

7.8.1.3. Connection to any IS within a SCIF must be approved by the ISSO in writing.

7.8.1.4. PED's with wireless, Radio Frequency (RF), Infrared (IR) technology, microphones, or recording capability will not be used unless these capabilities are turned off or physically disabled.

7.8.1.5. If approved, the PED and associated media must be transported and stored in a manner that affords security sufficient to preclude compromise of information, sabotage, theft, or tampering. Procedures for handling the PED in a SCIF must be available and provided to the user.

7.8.2. Handling Procedures. When it has been determined that the use of PED's is absolutely necessary to fulfill mission requirements, and the requirements set forth in paragraph 7.8.2., are satisfied, the following procedures must be implemented and followed:

7.8.2.1. The responsible organization must develop a case specific Standard Operating Procedure (SOP) and/or ensure procedures are addressed in the site Concept of Operations (CONOP). The following information must be considered and, where applicable, included in the SOP:

7.8.2.1.1. The SOP must include the organization and name of the ISSO and Special Security Officer (SSO) responsible for the issue and control of PED's.

7.8.2.1.2. Specific PED's (e.g. Laptop Computers) may be used to process classified information. In addition, these PED's may be granted approval to connect to IS on a case-by-case basis in writing by the ISSO. Specified PED's approved to process classified information must meet minimum technical security requirements.

7.8.2.1.3. All programs, equipment or data diskettes used with the PED must be marked with a label identifying the appropriate classification. Labeling exemption for operational security (OPSEC) requirements may be granted within local policy with DAA/DAA Rep/SCO concurrence.

7.8.2.1.4. If unauthorized classified information is identified on a PED, established procedures for handling suspected compromises shall be followed. For example, classified information on an unclassified PED may result in confiscation of the device as an incident.

7.8.2.1.5. Every effort should be made to ensure that security control features are implemented when possible (e.g., access control through userid/password).

7.8.2.2. Standard Operating Procedure (SOP) Approval. The organization requesting the use of PED's must submit the SOP to the ISSO/SSO for coordination and approval.

7.9. Contractor/Business owned PEDs. Work centers/units/individuals are responsible for ensuring compliance with this instruction by contractor or business representatives that they are sponsoring.

7.9.1. Non-government PEDs are prohibited for entry into AFSOC buildings where classified or controlled unclassified information is processed, stored, or discussed-no exceptions will be granted.

8. Waivers/Exceptions. Exceptions to this policy must be based on operation/mission need. The procedures for requesting an exception to this policy is to submit a PED Exception Request Form (Attachment 3) signed by commander/director to the respective information protection office (Wing/Major Command (MAJCOM)) for approval/disapproval. Prior to approval/disapproval, by the Wing/MAJCOM information protection office, requests will be coordinated with the corresponding Emission Security (EMSEC) office (Wing/MAJCOM). If a request is approved, a letter will be issued that must be carried by persons utilizing PEDs under the exception to policy. Exceptions will be specific in that they will authorize a specific person to operate a specific or multiple PED(s).

8.1. All EMSEC restrictions will be adhered to by those operating under exceptions to the PED policy. As a general rule, all devices with a RF signal will be kept 3 meters from classified processing devices.

8.2. First responders (e.g., Fire/Rescue, Security Forces), while executing emergency duties are automatically exempt and do not require an approved exception request to operate job related government PEDs in any AFSOC building where classified or controlled unclassified information is processed, stored, or discussed. However, they should attempt to minimize the duration of PED use.

VON A. GARDINER, Colonel, USAF
Director, Communications and Information

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

DODI 5200.1-R, *DOD Information Security Program and Protection of Sensitive Compartmented Information*, 9 Oct 2008

AFI 33-112, *Information Technology Hardware Asset Management*, 7 Apr 2006

AFI 33-219, *Telecommunications Monitoring and Assessment Program*, 1 May 2006

AFI 33-322, *Records Management Program*, 7 Oct 2003

AFMAN 33-223*, Identification and Authentication*, 6 July 2006

AFMAN 33-363*, Management of Records*, 8 Mar 2008

Prescribed Forms

None.

Adopted Forms

AF Form 847*, Recommendation for Change of Publication*

Abbreviations and Acronyms

AF—Air Force

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFSOC—Air Force Special Operations Command

AFRC—Air Force Reserve Command

AFRIMS—Air Force Records Information Management System

AFPD—Air Force Policy Directive

ANG—Air National Guard

ATO—Authority to Connect

BECO—Base Equipment Control Officer

CERT—Computer Emergency Response Team

CIO—Chief Information Officer

CONOPS—Concept of Operations

CONUS—Continental United States

CST—Client Systems Technician

CT—Cellular telephones

CTO—Certificate to Operate

DAA—Designated Approving Authorities

DIA—Defense Intelligence Agency

DISA—Defense Information Systems Agency

DOD—Department of Defense

EMSEC—Emission Security

FCC—Federal Communications Commission

GSM—Global System for Mobile Communications

GSUs—Geographically Separated Units

HQ AFSOC—Headquarters Air Force Special Operations Command

IR—Infrared

IS—Information Systems

ISSO—Information System Security Officers

ISP—Internet Service Provider

LAN—Local Area Network

LMR—Land Mobile Radios

MAJCOM—Major Command

OCONUS—Outside the Continental United States

OPSEC—Operations Security

OPR—Office of Responsibility

OWA—Outlook Web Access

NSA—National Security Agency

NTIA—National Telecommunications and Information Administration

PCMCIA—Personal Computer Memory Card International Association

PCs—Tablet Personal Computers

PDA—Personal Digital Assistants

PED—Portable Electronic Devices

SAP—Special Access Program

SAPF—Special Access Program Facility

SAR—Special Access Required

SCIF—Sensitive Compartmented Information Facilities

SIO—Senior Intelligence Officer

SME PED—Secure Mobile Environment Portable Electronic Device

SOP—Standard Operating Procedure

SSO—Special Security Office

STIG—Wireless Security Technical Implementation Guide

RAS—Remote Access Server

RDS—Records Disposition Schedule

RF—Radio Frequency

RIM—Research in Motion's

USSOCOM—United States Special Operations Command

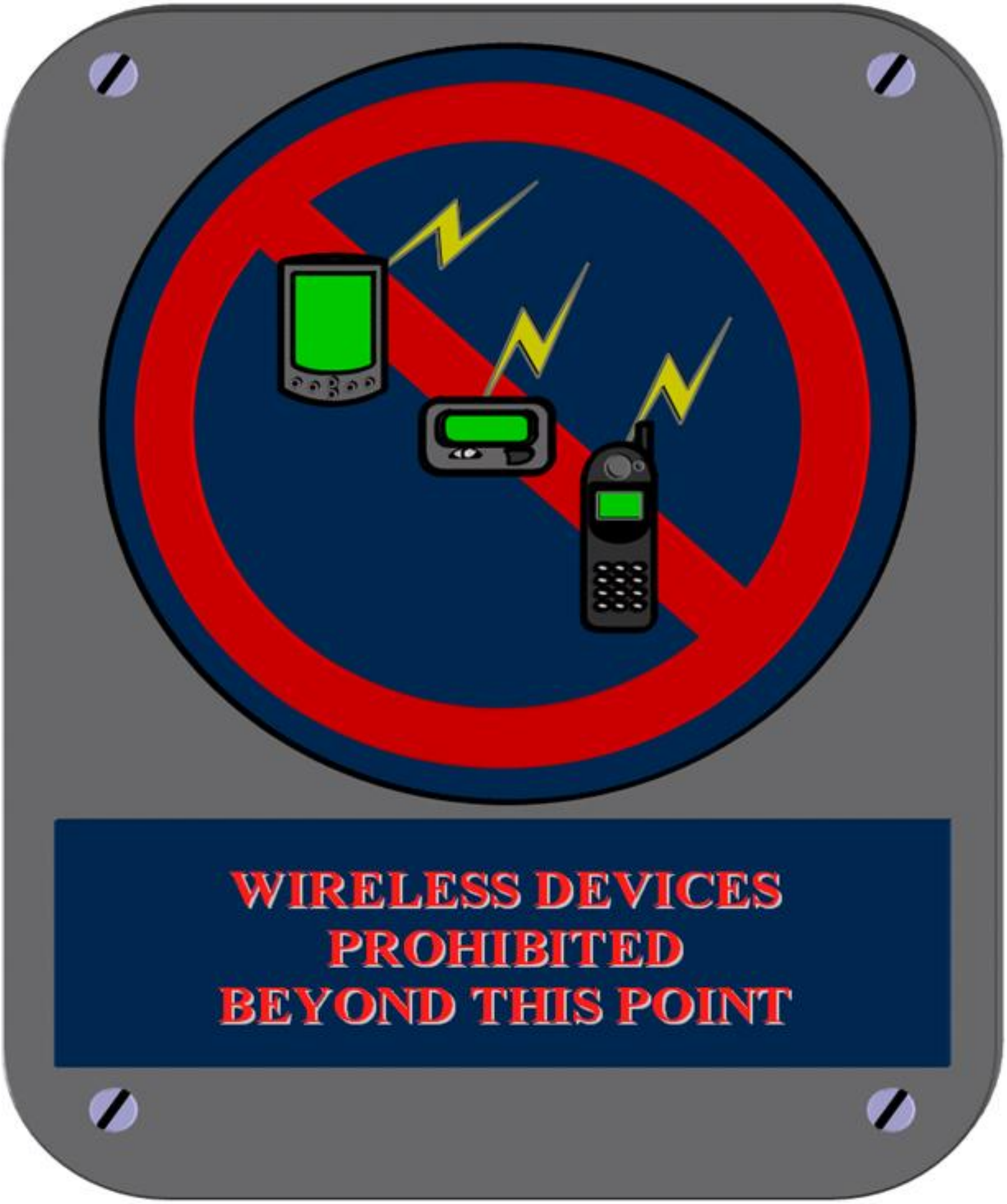
VPN—Virtual Private Network

WIAO—Wing Information Assurance Office

Attachment 2

SAMPLE ENTRY/EXIT POINT SIGN

Figure A2.1. Sample Entry/Exit Point Sign.



Attachment 3

SAMPLE PORTABLE ELECTRONIC DEVICE (PED) SECURITY TRAINING INFORMATION

A3.1. Overview. Although Portable Electronic Devices (PEDs) provide users more efficient ways of accomplishing work, many of the inherent features of the devices, when used improperly, can lead to the unauthorized discloser of sensitive or classified information. The information below includes excerpts from recent National Security Agency (NSA) advisories highlighting the major security issues with PEDs.

A3.2. Security Risks. The introduction or use of PEDs in areas where classified information may be discussed or processed should be carefully managed and controlled. In order to increase functionality and user convenience, today's PEDs include built-in features such as infrared (IR), radio frequency (RF), audio recording, and telephone modem communication capabilities. These same features, which are implemented to allow easy connectivity between a PED and other devices for performing data exchanges, along with their expanded memory and processing ability, create new avenues for potential attacks. Attempts to temporarily disable these features by external means may not actually be solutions and, in some cases, may even increase risk from the associated vulnerabilities. Some of the features that pose the greatest risk to information or information systems in a classified environment include:

A3.3. Infrared (IR) Ports. Since most units are capable of both sending and receiving data without indication to the user, this feature poses a high security risk and should always be disabled as a default measure. Simply covering the IR emitter/detector with an opaque covering is not adequate due to variability in effectiveness and inability to readily determine the characteristics of the covering by simple visual inspection. The only tape shown to be effective in preventing unauthorized activity through the IR port is metallic tape, such as aluminum or copper foil tape.

A3.4. Wireless Radio Frequency (RF) Communications. This capability is normally provided in one of two ways: Wireless local area network (LAN) or cell-phone type medium-speed data access. The frequency ranges of these two systems differ, as do the data rates and therefore the quantity of data that can be transmitted and received in a given period of time. In both cases, the data handling capabilities are nontrivial and present a security risk. Removal of the antenna is not a suitable countermeasure to eliminate RF operations, since some systems can communicate with the antenna removed. In some cases, removal of the antenna requires the antenna to be raised, which activates the RF transceiver.

A3.5. Backdoors. Unauthorized wireless solutions may create backdoors into LANs. If a device receives information via an unapproved wireless technology and that device allows that information to be placed directly into the LAN at the workstation level, then all perimeter and host-based security devices have been bypassed.

A3.6. Electromagnetic Radiation. The electromagnetic radiation from the device can allow the user to be geolocated. Wireless PEDs are susceptible to interference, interception, and can be jammed. When using wireless PEDs, Operational Security (OPSEC) and force protection should be a compelling consideration.

A3.7. Additional Security Concerns. The following areas also cause familiar security concerns in PEDs and need to be recognized and handled consistent with existing security policies and procedures.

A3.8. Removable Peripheral/Expansion Devices [e. g., Personal Computer Memory Card International Association (PCMCIA) and Smart Card devices]. Many expansion cards in this category have independent processing capability from the host equipment and therefore may create vulnerabilities even where none are present in the host unit.

A3.9. Audio Recording Capability. Some of these devices are capable of recording up to six hours of audio. Additionally, some microphones are capable of picking up normal office conversation from a distance in excess of 50 feet. Vulnerabilities from this capability should be well understood and appreciated. While much emphasis is placed on the audio recording capabilities of handheld devices, most laptop computers also organically provide audio recording capabilities that must be understood and properly configured to avoid unintentional compromise.

A3.10. Ease of Upgrade and Availability. An extensive library of programs has allowed users to have access to software features such as operating system extensions, utilities, and built-in features. These programs were created for users to configure their PEDs to their liking, but they also allow easy staging of attacks. Users should be aware that malicious code could just as easily be uploaded.

A3.11. Connectivity of external device applications such as external modems and IR hubs. External modems left connected to a phone system, whether live or idle, may allow a covert connection to an external source. Connections to a phone network should never be left unattended. IR hubs may open an easy route of attack. PEDs and other devices should not be left connected via IR for extended periods of time as an external party could gain access remotely. Care should be taken to not only guard against unauthorized access to the PED, but also devices that may connect or download via IR.

A3.12. Remote configuration and activation. Many cell phones can be remotely configured and powered-on by the cellular telephone service provider. This capability can be exploited by an adversary to gain access to sensitive or classified conversations.

A3.13. Remote Viewing. Techniques exist that permit an adversary to view what is displayed on the PDA screen from greater than expected distances. Users are cautioned not to display classified data on their PED when in the vicinity of untrusted parties.